BUNDESREPUBLIK DEUTSCHLAND

Bescheinigung

Die Francotyp-Postalia AG & Co in Birkenwerder/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Sicherheitsmodul und Verfahren zur Sicherung der Postregister vor Manipulation"

am 15. Juni 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 07 B und G 06 F der Internationalen Patentklassifikation erhalten.

München, den 28. März 2000

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Ebert

Aktenzeichen: 199 28 057.6

A 9161
06.90
11/98

Francotyp-Postalia AG & Co.
Triftweg 21 - 26
16547 Birkenwerder

15. Juni 1999

3151-DE

Sicherheitsmodul und Verfahren zur Sicherung der Postregister vor Manipulation

---

Beschreibung

Die Erfindung betrifft ein Sicherheitsmodul mit Sicherung der Postregister vor Manipulation, gemäß der im Oberbegriff des Anspruchs 1 angegebenen Art und für ein Verfahren zur Sicherung der Postregister vor Manipulation gemäß der im Oberbegriff des Anspruchs 10 angegebenen Art. Ein solcher postalischer Sicherheitsmodul ist insbesondere für den Einsatz in einer Frankiermaschine bzw. Postbearbeitungsmaschine oder Computer mit Postbearbeitungsfunktion geeignet.

Es sind vielfältige Sicherungsmaßnahmen zum Schutz gegen Ausfälle bzw. Störungen von intelligenten elektronischen Systemen bekannt.

Es ist bereits aus EP 417 447 B1 bekannt, in elektronischen Datenverarbeitungsanlagen besondere Module einzusetzen und mit Mitteln zum Schutz vor einem Einbruch in ihre Elektronik auszustatten. Solche Module werden nachfolgend Sicherheitsmodule genannt.

Moderne Frankiermaschinen, oder andere Einrichtungen zum Frankieren von Postgut, sind mit einem Drucker zum Drucken des Postwertstempels auf das Postgut, mit einer Steuerung zum Steuern des Druckens und der peripheren Komponenten der Frankiermaschine, mit einer Abrecheneinheit zum Abrechnen von Postgebühren, die in nichtflüchtigen Speichern gehalten werden, und einer Einheit zum kryptografischen Absichern der Postgebührendaten ausgestattet. Ein Sicherheitsmodul (EP 789 333 A2) kann eine Hardware-Abrecheneinheit und/oder die Einheit zum Absichern des Druckens der Postgebührendaten aufweisen. Beispielsweise kann ersterer als Anwenderschaltkreis ASIC und letzterer als OTP-Prozessor (One Time Programmable) realisiert werden. Der interne OTP-ROM speichert auslesesicher sensible Daten (kryptografische Schlüssel), die beispielsweise zum Nachladen eines Guthabens erforderlich sind. Eine Kapselung durch ein Sicherheitsgehäuse bietet einen weiteren Schutz.

Weitere Maßnahmen zum Schutz eines Sicherheitsmoduls vor einem Angriff auf die in ihm gespeicherten Daten wurden auch in den nicht vorveröffentlichten deutschen Anmeldungen 198 16 572.2 8 mit dem Titel: Anordnung für ein Sicherheitsmodul und 198 16 571.4 mit dem Titel: Anordnung für den Zugriffsschutz für Sicherheitsmodule, sowie 199 12 780. 8 mit dem Titel: Anordnung für ein Sicherheitsmodul, 199 12 781.6 mit dem Titel: Verfahren zum Schutz eines Sicherheitsmoduls und Anordnung zur Durchführung des Verfahrens und die deutsche Gebrauchsmusteranmeldung 299 05 219.2 mit dem Titel: Sicherheitsmodul mit Statussignalisierung vorgeschlagen. Ein steckbares Sicherheitsmodul kann in seinem Lebenszyklus verschiedene Zustände einnehmen. Es kann nun unterschieden werden, ob das Sicherheitsmodul funktioniert oder defekt ist. Dabei wird auf die Nichtmanipulierbarkeit der hardwaremäßigen Abrechnung vertraut, ohne dies noch einmal zu kontrollieren. Jede andere softwaregesteuerte Arbeitsweise gilt nur mit den Orginalprogrammen als fehlerfrei, welche deshalb vor einer Manipulation geschützt werden müssen.

Bekanntlich wird in Frankiermaschinen, beispielsweise vom Typ T1000, ein MAC (MESSAGE AUTHENTIFICATION CODE) zur Absicherung der

Postregisterdaten eingesetzt (EP 762 338 A2, US 5,805,711). Auf diese Weise kann auch der Mikroprozessor des Sicherheitsmoduls vor einer Abrechnung die Gültigkeit (Manipulationsfreiheit) der Postregister überprüfen. Der Mikroprozessor berechnet einen MAC über die Daten in den Postregistern und vergleicht diesen MAC mit einem Vergleichs-MAC der für diese Postregister bereits früher gespeichert worden ist. Anschließend erfolgt eine Abrechnung. Danach muß der Mikroprozessor erneut den Vergleichs-MAC für die vom Anwenderschaltkreis ASIC modifizierten Postregister berechnen, um ihn zu aktualisieren. In dieser Zeit, vom Start der Abrechnung bis zum Schreiben des neuen Vergleichs-MAC, sind jedoch für einen Betrüger mit Speicherzugriff die Postregister manipulierbar, ohne daß dies durch den Mikroprozessor erkannt werden kann.

Der Erfindung liegt die Aufgabe zugrunde, für ein Sicherheitsmodul die Sicherheit bei der Abrechnung zu erhöhen.

Es soll ein Verfahren gefunden werden, welches mit minimalen Aufwänden eine maximale Sicherheit vor einer Manipulation der gespeicherten Daten ermöglicht. Das Verfahren soll beispielsweise in Frankiermaschinen Anwendung finden, für die besondere Sicherheitsforderungen bezüglich der Postregisterdaten gelten, da insbesondere die geldwerten Abrechnungsdaten unmanipulierbar sein müssen.

Die Aufgabe wird mit den Merkmalen des Anspruchs 1 für eine Anordnung und mit den Merkmalen des Anspruchs 10 für ein Verfahren gelöst.

Eine Lösung des Problems wurde in der Durchführung von zwei zeitlich versetzten Abrechnungen durch unterschiedliche Rechner gefunden.

Voraussetzung für eine Vorausberechnung eines Postregistersatzes ist ein schon zu Beginn vorliegender Authorisierungscode (MAC_{alt}), der die Gültigkeit eines vorherigen Postregistersatzes und damit der vorherigen Abrechnungsdaten in an sich bekannter Weise zu überprüfen gestattet. Bei deren Gültigkeit wird von dem ersten Rech-ner eine Vorausberechnung eines zugehörigen Authorisierungscode (MAC_{neu}) über den

vorausberechneten Postregistersatz vorgenommen. Vorzugsweise wird hierzu ein Mikroprozessor eines Sicherheitsmoduls eingesetzt, welcher nachfolgend als Modulcomputer bezeichnet wird. Wenn der Modulcomputer, beispielsweise vor Beginn der Vorausabrechnung, den alten Postregistersatz durch Berechnung eines MAC´s und durch den Vergleich dieses MAC´s mit dem gespeicherten MAC_{alt} überprüft hat, berechnet er im sicheren Speicherbereich den für die nächste Abrechnung zugehörigen neuen Authorisierungscode MAC_{neu} im voraus, bevor die Hauptabrechung angestoßen wird, die ein zweiten Rechner durchführt. Vorzugsweise wird hierzu eine anwenderspezifische Verarbeitungseinheit ASIC des Sicherheitsmoduls eingesetzt, welches eine Hardwareabrechnungsbaugruppe aufweist und die Abrechnungsdaten in die Postregister einschreibt. Zum Abschluß der Hauptabrechnung speichert der Modulcomputer nun noch den vorab berechneten MAC_{neu} als aktuellen gültigen MAC zu dem Postregistersatz mit den aktuellen Abrechnungsdaten. Der Unterschied liegt also:

1. im Zeitpunkt der MAC-Berechnung vor der Hauptabrechnung,
2. in der Quelle der MAC-Berechnung, weil dazu vom Modulcomputer zuerst die Postregisterabrechnungsdaten für den MAC_{neu} vorausberechnet werden müssen.

Wenn die nächste Abrechnung erfolgt, wird das o.g. Verfahren wiederholt. Mit dem erfindungsgemäßen Verfahren kann durch das Prüfen der MAC´s nun auch eine während der Abrechnung vorgenommene Manipulation festgestellt werden. Da die Quellen für die MAC-Berechnung der beiden Vergleichswerte unterschiedlich sind, müssen die zu vergleichenden MAC´s identisch sind. Unter der Annahme, daß bei der Abrechnung durch das ASIC kein Fehler auftritt, kann es sich nur um eine Manipulation handeln, wenn die MAC´s nicht übereinstimmen.

Ein weiterer Vorteil dieser Methode ist der, daß beim Einschalten (PowerOn) zwei MAC´s existieren.

1. einer, der für die Postregister gilt, falls die Abrechnung nicht vollständig beendet wurde
2. einer, der für die Postregister gilt, falls die Abrechnung beendet wurde, der neue MAC aber noch nicht geschrieben werden konnte.

Somit muß mindestens ein Postregistersatz existieren, dessen MAC mit einem dieser beiden übereinstimmt. Letzterer ist der gültige nicht manipulierte Registersatz und kann als Referenz gelten. Andernfalls wurde manipuliert.

Diese Methode sichert zu jedem Zeitpunkt t die Postregisterdaten mit einem MAC. Ein Angriff durch eine Manipulation der Registerdaten zu einem beliebigen Zeitpunkt kann nicht mehr unbemerkt bleiben.

Ein Sicherheitsmodul für beispielsweise eine Frankiermaschine, nimmt deren Funktion einer Abrechnung war, insbesondere von Postgebühren und/oder deren kryptografische Absicherung. Es ist erfindungsgemäß durch eigene Signalmittel gekennzeichnet, die bei direkter Ansteuerung vom Prozessor des Sicherheitsmoduls eine Aussage über den aktuellen Zustand des Sicherheitsmoduls gestatten. Die Signalisierung des Modulzustandes wird nur bei Versorgung des Sicherheitsmoduls mit Systemspannung aktiviert, um eine Batterie zu schonen. Der Prozessor überwacht die hardwaremäßige Abrecheneinheit. Dabei steht nicht die Verfügbarkeit des Systems im Vordergrund, sondern die sichere Erkennung von Fehlfunktionen oder Ausfällen sowie eine geeignete Reaktion darauf, wie es bei besonders sicherheitssensitiven, eher zeitunkritischen Vorgängen der Fall ist.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Figur 1, Perspektivische Ansicht der Frankiermaschine von hinten,

Figur 2, Blockschaltbild des Sicherheitsmoduls,

Figur 3, Seitenansicht des Sicherheitsmoduls,

Figur 4, Draufsicht auf das Sicherheitsmodul,

Figur 5, Tabelle für Statussignalisierung,

Figur 6, Darstellung der Prüfungen im System für statische und dynamisch änderbare Zustände,

Figur 7, Darstellung von Abläufen bei der Abrechnung anhand eines Zeitstrahles,

Figur 8, Flußdiagramm für die Prüfungen des Systems vor dem Frankieren.

In der Figur 1 ist eine perspektivische Ansicht der Frankiermaschine von hinten dargestellt. Die Frankiermaschine besteht aus einem Meter 1 und einer Base 2. Letztere ist mit einer Chipkarten-Schreib/ Leseeinheit 70 ausgestattet, die hinter der Führungsplatte 20 angeordnet und von der Gehäuseoberkante 22 zugänglich ist. Nach dem Einschalten der Frankiermaschine mittels dem Schalter 71 wird eine Chipkarte 49 von oben nach unten in den Einsteckschlitz 72 eingesteckt. Ein zugeführter auf der Kante stehender Brief 3, der mit seiner zu bedruckenden Oberfläche an der Führungsplatte anliegt, wird dann entsprechend der Eingabedaten mit einem Frankierstempel 31 bedruckt. Die Briefzuführöffnung wird durch eine Klarsichtplatte 21 und die Führungsplatte 20 seitlich begrenzt.

Das Modul wird auf die Hauptplatine des Meters der Frankiermaschine oder eines anderen geeigneten Gerätes gesteckt. Es ist vorzugsweise innerhalb des Metergehäuses untergebracht, welches als Sicherheitsgehäuse ausgebildet ist. Das Metergehäuse ist dabei vorteilhaft so

konstruiert, daß der Benutzer die Statusanzeige des Sicherheitsmoduls trotzdem von außen durch eine Öffnung 109 sehen kann, wobei sich die Öffnung 109 zur Bedienoberfläche 88, 89 des Meters 1 erstreckt.

Die Anzeige wird direkt vom modulinternen Prozessor gesteuert und ist so von außen nicht ohne weiteres manipulierbar. Die Anzeige ist im Betriebszustand ständig aktiv, so daß das Anlegen der Systemspannung Us+ an den Prozessor des Sicherheitsmoduls ausreicht, die Anzeige zu aktivieren, um den Modulzustand ablesen zu können.

Die Figur 2 zeigt ein Blockschaltbild des postalischen Sicherheitsmoduls PSM 100 in einer bevorzugten Variante. Der negative Pol der Batterie 134 ist auf Masse und einen Pin P23 der Kontaktgruppe 102 gelegt. Der positive Pol der Batterie 134 ist über die Leitung 193 mit dem einen Eingang des Spannungsumschalters 180 und die Systemspannung führende Leitung 191 ist mit dem anderen Eingang des Spannungsumschalters 180 verbunden. Als Batterie 134 eignet sich der Typ SL-389/P für eine Lebensdauer bis zu 3,5 Jahren oder der Typ SL-386/P für eine Lebensdauer bis zu 6 Jahren bei einem maximalen Stromverbrauch durch das PSM 100. Als Spannungsumschalter 180 kann ein handelsüblicher Schaltkreis vom Typ ADM 8693ARN eingesetzt werden. Der Ausgang des Spannungsumschalters 180 liegt über die Leitung 136 an einer Spannungsüberwachungseinheit 12 und einer Detektionseinheit 13 an. Die Spannungsüberwachungseinheit 12 und die Detektionseinheit 13 stehen mit den Pins1, 2, 4 und 5 des Prozessors 120 über die Leitungen 135, 164 und 137, 139 in Kommunikationsverbindung. Der Ausgang des Spannungsumschalters 180 liegt über die Leitung 136 außerdem am Versorgungseingang eines ersten Speichers SRAM an, der durch die vorhandene Batterie 134 zum nichtflüchtigen Speicher NVRAM 116 einer ersten Technologie wird.

Das Sicherheitsmodul steht mit der Frankiermaschine über den Systembus 115,117, 118 in Verbindung. Der Prozessor 120 kann über den Systembus und ein Modem 83 in Kommunikationsverbindung mit einer entfernten Datenzentrale eintreten. Die Abrechnung wird vom ASIC

150 vollzogen. Die postalischen Abrechnungsdaten werden in nichtflüchtigen Speichern unterschiedlicher Technologie gespeichert.
Am Versorgungseingang eines zweiten Speichers NV-RAM 114 liegt Systemspannung an. Hierbei handelt es sich um einen nichtflüchtigen Speicher NVRAM einer zweiten Technologie, (SHADOW-RAM). Diese zweiten Technologie umfaßt vorzugsweise ein RAM und ein EEPROM, wobei letzteres die Dateninhalte bei Systemspannungsausfall automatisch übernimmt. Der NVRAM 114 der zweiten Technologie ist mit den entsprechenden Adress- und Dateneingängen des ASIC´s 150 über einen internen Adreß- und Datenbus 112, 113 verbunden.

Der ASIC 150 enthält mindestens eine Hardware-Abrecheneinheit für die Berechnung der zu speichernden postalischen Daten. In der Programmable Array Logic (PAL) 160 ist eine Zugriffslogik für den ASIC 150 untergebracht. Der ASIC 150 wird durch die Logik PAL 160 gesteuert. Ein Adreß- und Steuerbus 117, 115 von der Hauptplatine des Meters 1 ist an entsprechenden Pins der Logik PAL 160 angeschlossen und die PAL 160 erzeugt mindestens ein Steuersignal für das ASIC 150 und ein Steuersignal 119 für den Programmspeicher FLASH 128. Der Prozessor 120 arbeitet ein Programm ab, das im FLASH 128 gespeichert ist. Der Prozessor 120, FLASH 28, ASIC 12 und PAL 160 sind über einen modulinternen Systembus miteinander verbunden, der Leitungen 110,111,126,119 für Daten-, Adreß- und Steuersignale enthält.

Die RESET-Einheit 130 ist über die Leitung 131 mit dem Pin 3 des Prozessors 120 und mit einem Pin des ASIC´s 150 verbunden. Der Prozessor 120 und das ASIC 150 werden bei Absinken der Versorgungsspannung durch eine Resetgenerierung in der RESET-Einheit 130 zurückgesetzt.

Der Prozessor 120 weist intern eine Verarbeitungseinheit CPU 121, eine Echtzeituhr RTC 122 eine RAM-Einheit 124 und eine Ein/Ausgabe-Einheit 125 auf. Der Prozessor 120 des Sicherheitsmoduls 100 ist über einen

modul-internen Datenbus 126 mit einem FLASH 128 und mit dem ASIC 150 verbunden. Der FLASH 128 dient als Programmspeicher und wird mit Systemspannung Us+ versorgt. Er ist beispielsweise ein 128 Kbyte-FLASH-Speicher vom Typ AM29F010-45EC. Der ASIC 150 des postalischen Sicherheitsmoduls 100 liefert über einen modulinternen Adreßbus 110 die Adressen 0 bis 7 an die entsprechenden Adreßeingänge des FLASH 128. Der Prozessor 120 des Sicherheitsmoduls 100 liefert über einen internen Adreßbus 111 die Adressen 8 bis 15 an die entsprechenden Adresseingänge des FLASH 128. Der ASIC 150 des Sicherheitsmoduls 100 steht über die Kontaktgruppe 101 des Interfaces mit dem Datenbus 118, mit dem Adreßbus 117 und dem Steuerbus 115 der Hauptplatine des Meters 1 in Kommunikationsverbindung.

Der Spannungsumschalter 180 gibt als Ausgangsspannung auf der Leitung 136 für die Spannungsüberwachungseinheit 12 und Speicher 116 diejenige seiner Eingangsspannungen weiter, die größer als die andere ist. Durch die Möglichkeit, die beschriebene Schaltung in Abhängigkeit von der Höhe der Spannungen Us+ und Ub+ automatisch mit der größeren von beiden zu speisen, kann während des Normalbetriebs die Batterie 134 ohne Datenverlust gewechselt werden. Die Echtzeituhr RTC 122 und der Speicher RAM 124 werden von einer Betriebsspannung über die Leitung 138 versorgt. Diese Spannung wird von der Spannungsüberwachungseinheit 12 erzeugt.

Die Batterie der Frankiermaschine speist in den Ruhezeiten außerhalb des Normalbetriebes in vorerwähnter Weise die Echtzeituhr 122 mit Datums und/oder Uhrzeitregistern und/oder den statischen RAM (SRAM) 124, der sicherheitsrelevante Daten hält. Sinkt die Spannung der Batterie während des Batteriebetriebs unter eine bestimmte Grenze, so wird von der Schaltung 12 der Speisepunkt für RTC und SRAM mit Masse verbunden. Das heißt, die Spannung an der RTC und am SRAM liegt dann bei 0V. Das führt dazu, daß der SRAM 124, der z.B. wichtige kryptografische Schlüssel enthält, sehr schnell gelöscht wird. Gleichzeitig

werden auch die Register der RTC 122 gelöscht und die aktuelle Uhrzeit und das aktuelle Datum gehen verloren. Durch diese Aktion wird verhindert, daß ein möglicher Angreifer durch Manipulation der Batteriespannung die frankiermaschineninterne Uhr 122 anhält, ohne daß sicherheitsrelevante Daten verloren gehen. Somit wird verhindert, daß er Sicherheitsmaßnahmen, wie beispielsweise Sleeping Mode (EP 660 268 A2) oder Long Time Watchdog (wird anhand der Fig.5 noch erläutert) umgeht.

Die Schaltung der Spannungsüberwachungseinheit 12 ist beispielsweise so dimensioniert, daß jegliches Absinken der Batteriespannung auf der Leitung 136 unter die spezifizierte Schwelle von 2,6 V zum Ansprechen der Schaltung 12 führt. Gleichzeitig mit der Indikation der Unterspannung der Batterie wechselt die Schaltung 12 in einen Selbsthaltezustand, in dem sie auch bei nachträglicher Erhöhung der Spannung bleibt. Sie liefert außerdem ein Statussignal 164. Beim nächsten Einschalten des Moduls kann der Prozessor den Zustand der Schaltung abfragen (Statussignal) und damit und/oder über die Auswertung der Inhalte des gelöschten Speichers darauf schließen, daß die Batteriespannung zwischenzeitlich einen bestimmten Wert unterschritten hat. Der Prozessor kann die Überwachungsschaltung 12 zurücksetzen, d.h. "scharf" machen. Letztere reagiert auf ein Steuersignal auf der Leitung 135.

Die Leitung 136 am Eingang des Batterieobservers 12 versorgt zugleich eine Detektions-Einheit 13 mit Betriebs- oder Batteriespannung. Vom Prozessor 120 wird der Zustand der Detektions-Einheit 13 über die Leitung 139 abgefragt oder die Detektions-Einheit 13 wird vom Prozessor 120 über die Leitung 137 ausgelöst bzw. gesetzt. Nach dem Setzen wird eine statische Prüfung auf Anschluß durchgeführt. Dazu wird über eine Leitung 192 Massepotential abgefragt, welches am Anschluß P4 des Interfaces des postalischen Sicherheitsmoduls PSM 100 anliegt und nur abfragbar ist, wenn der Sicherheitsmodul 100 ordnungsgemäß gesteckt ist. Bei gesteckten Sicherheitsmodul 100 wird Massepotential des negativen Pols 104 der Batterie 134 des postalischen Sicherheitsmoduls

PSM 100 auf den Anschluß P23 des Interfaces 8 gelegt und ist somit am Anschluß P4 des Interfaces über die Leitung 192 von der Detektions-Einheit 13 abfragbar.

An den Pins 6 und 7 des Prozessors 120 sind Leitungen angeschlossen, welche nur bei einem, beispielsweise an die Hauptplatine des Meters 1, gesteckten Sicherheitsmodul 100 eine Leiterschleife 18 bilden. Zur dynamischen Prüfung des Angeschlossenseins des postalischen Sicherheitsmoduls PSM 100 an der Hauptplatine des Meters 1 werden vom Prozessor 120 wechselnde Signalpegel in ganz unregelmäßigen Zeitabständen an die Pin´s 6, 7 angelegt und über die Schleife zurückgeschleift.

Der Prozessor 120 ist mit der Ein/Ausgabe-Einheit 125 ausgestattet, deren Anschlüsse Pin´s 8, 9 zur Ausgabe mindestens eines Signals zur Signalisierung des Zustandes des Sicherheitsmoduls 100 dienen. An den Pin´s 8 und 9 liegen I/O-Ports der Ein/Ausgabe-Einheit 125, an welchen modulinterne Signalmittel angeschlossen sind, beispielsweise farbige Lichtemitterdioden LED´s 107, 108. Diese signalisieren den Modulzustand bei einem auf die Hauptplatine des Meters 1 gesteckten Sicherheits-moduls 100 durch eine Öffnung 109 im Metergehäuse. Die Sicherheits-module können in ihrem Lebenszyklus verschiedene Zustände ein-nehmen. So muß z.B. detektiert werden, ob das Modul gültige kryptografische Schlüssel enthält. Weiterhin ist es auch wichtig zu unterscheiden, ob das Modul funktioniert oder defekt ist. Die genaue Art und Anzahl der Modulzustände ist von den realisierten Funktionen im Modul und von der Implementierung abhängig.

Die Figur 3 zeigt zeigt den mechanischen Aufbau des Sicherheitsmoduls in Seitenansicht. Das Sicherheitsmodul ist als Multi-Chip-Modul ausge-bildet, d.h. mehrere Funktionseinheiten sind auf einer Leiterplatte 106 verschaltet. Das Sicherheitsmodul 100 ist mit einer harten Vergußmasse 105 vergossen, wobei die Batterie 134 des Sicherheitsmoduls 100 außerhalb der Vergußmasse 105 auf einer Leiterplatte 106 auswech-

selbar angeordnet ist. Beispielsweise ist es so mit einem Vergußmaterial 105 vergossen, daß das Signalmittel 107, 108 aus dem Vergußmaterial an einer ersten Stelle herausragt und daß die Leiterplatte 106 mit der gesteckten Batterie 134 seitlich einer zweiten Stelle herausragt. Die Leiterplatte 106 hat außerdem Batteriekontaktklemmen 103 und 104 für den Anschluß der Pole der Batterie 134, vorzugsweise auf der Bestückungsseite oberhalb der Leiterplatte 106. Es ist vorgesehen, daß zum Anstecken des postalischen Sicherheitsmoduls PSM 100 auf die Hauptplatine des Meters 1 die Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 (Leiterbahnseite) des Sicherheitsmoduls 100 angeordnet sind. Der Anwenderschaltkreis ASIC 150 steht über die erste Kontaktgruppe 101 - in nicht gezeigter Weise - mit dem Systembus einer Steuereinrichtung 1 in Kommunikationsverbindung und die zweite Kontaktgruppe 102 dient der Versorgung des Sicherheitsmoduls 100 mit der Systemspannung. Wird das Sicherheitsmodul auf die Hauptplatine gesteckt, dann ist es vorzugsweise innerhalb des Metergehäuses dergestalt angeordnet, so daß das Signalmittel 107, 108 nahe einer Öffnung 109 ist oder in diese hineinragt. Das Metergehäuse ist damit vorteilhaft so konstruiert, daß der Benutzer die Statusanzeige des Sicherheitsmoduls trotzdem von außen sehen kann. Die beiden Leuchtdioden 107 und 108 des Signalmittels werden über zwei Ausgangssignale der I/O-Ports an den Pin 8, 9 des Prozessors 120 gesteuert. Beide Leuchtdioden sind in einem gemeinsamen Bauelementegehäuse untergebracht (Bicolorleuchtdiode), weshalb die Abmaße bzw. der Durchmesser der Öffnung relativ klein bleiben kann und in der Größenordnung des Signalmittels liegt. Prinzipiell sind drei unterschiedliche Farben darstellbar (rot, grün, orange), jenachdem die LED´s einzeln oder gleichzeitig angesteuert werden. Zur Zustandsunterscheidung werden die LED´s auch einzeln oder zusammen blinkend ggf. abwechseln blinkend gesteuert, so daß neun verschiedene Zustande unterschieden werden können, in welchem mindestens eine der LED´s aktiviert wird.

In der Figur 4 ist eine Draufsicht auf das postalische Sicherheitsmodul dargestellt. Die Vergußmasse 105 umgibt quaderförmig einen ersten Teil der Leiterplatte 106, während ein zweiter Teil der Leiterplatte 106 für die auswechselbar angeordnete Batterie 134 von Vergußmasse frei bleibt. Die Batteriekontaktklemmen 103 und 104 werden hier von der Batterie verdeckt.

Gemäß einer in der Figur 5 gezeigten - sich selbst erläuternden - Tabelle für Statussignalisierung geht eine Vielzahl möglicher Zustandsanzeigen hervor. Eine grün leuchtende LED 107 signalisiert einen OK-Zustand 220, aber eine leuchtende LED 108 signalisiert einen Fehler-Zustand 230 im Ergebnis eines mindestens statischen Selbsttestes. Das Ergebnis eines solchen an sich bekannten Selbsttestes kann wegen der direkten Signalisierung über die LED´s 107, 108 nicht verfälscht werden.
Beispielsweise für den Fall, daß zwischenzeitlich die im Sicherheitsmodul gespeicherten Schlüssel verlohren gingen, würde die laufende Überprüfung im dynamischen Betrieb den Fehler feststellen und als den Zustand 240 mit orange leuchtenden LED´s signalisieren. Nach einem Aus/Einschalten ist ein Booten erforderlich, da anderenfalls keine andere Operation mehr ausgeführt werden kann. Der Fall, daß bei der Herstellung die Installation eines Schlüssels vergessen wurde, wird als Zustand 260 beispielsweise mit einer grün blinkenden LED 107 signalisiert. Auch der Fall, daß ein long time watchdog-Timer abgelaufen ist, wird als Zustand 250 durch eine rot blinkende LED signalisiert. Der long time watchdog-Timer ist abgelaufen, wenn lange Zeit die Datenzentrale nicht mehr kontaktiert wurde, beispielsweise um ein Guthaben nachzuladen. Der Zustand 250 wird ebenfalls erreicht, wenn das Sicherheitsmodul vom Meter getrennt wurde. Weitere Zustandsanzeigen für die Zustände 270, 280, 290 sind optional für verschiedene weitere Prüfungen vorgesehen.

Die Figur 6 zeigt eine Darstellung der Prüfungen im System für statisch und dynamisch änderbare Zustände. Ein ausgeschaltetes System im Zustand 200 geht nach dem Einschalten über die Transition Start 201 in den Zustand 210 über, in welchem vom Sicherheitsmodule ein statischer Selbsttest durchgeführt wird sobald die Betriebsspannung anliegt. Bei der Transition 202, bei der der Selbsttest ein OK bei ordnungsgemäßem Ergebnis ergibt, wird der Zustand 220 LED grün leuchtend erreicht. Ausgehend von letzterem Zustand ist bei Bedarf ein wiederholter statischer Selbsttest und ein dynamischer Selbsttest durchführbar. Eine solche Transition 203 oder 206 führt entweder zurück auf den Zustand 220 LED grün bei OK oder auf den Zustand 240 LED orange bei einem Fehler. Letzterer ist durch einen Recover-Versuch evtl. durch Ausschalten (Transition 211) und Wiedereinschalten des Gerätes (Transition 201) behebbar. Statische Fehler sind aber nicht behebbar. Von Zustand 210, in welchem das eingeschaltete Gerät einen statischen Selbsttest ausführt, existiert bei einem Fehler eine Transition 204 zum Zustand 230 LED rot. Zu jeder Zeit, wenn sich das Gerät im Zustand 220 LED grün befindet, kann ein on demand ausgeführter statischer Selbsttest bei einem Fehler über eine Transition 205 zum Zustand 230 LED rot führen. Ausgehend vom Zustand 220 LED grün können nicht gezeigte weitere Transitionen 207, 208, 209 zu den weiteren Zuständen 270 (mit orange blinkenden LED´s signalisiert), 280 (mit rot leuchtend/orange blinkenden LED´s signalisiert) und 290 (mit grün leuchtend/orange blinkenden LED´s signalisiert) führen.

Der – in der Figur 2 gezeigte - Sicherheitsmodul 100 ist mit einem Programmspeicher 128, der ein Programm zur Sicherung der Postregister vor Manipulation aufweist, einer ersten und zweiten Datenverarbeitungseinheit 120, 150, mit nichtflüchtigen Speichern 114, 116, mit weiteren miteinander verschalteten Funktionseinheiten 12, 13, 130, 160 und 180 verbunden, wobei sämtliche vorgenannte Funktionseinheiten mit einer Vergußmasse 105 bedeckt sind, außer die Batterie 134 (Figuren 3 und 4). Im Sicherheitsmodul 100 ist die erste Datenverarbeitungseinheit 120 der

Modulprozessor. Letzterer ist für die Durchführung von mindestens einer Authorisierungsroutine für die Postregisterdaten programmiert, wobei deren Authorisierung in Verbindung mit dem zugehörigen Authorisierungscode MAC im nichtflüchtigen Speichern 114, 116 einen Modulzustand signalisiert, welcher eine weitere Abrechnung durchzuführen gestattet, und wobei zur Signalisierung des Modulzustandes ein optisches oder akustisches Signalmittel 107, 108 am Modulprozessor angeschlossen ist. Die erste Datenverarbeitungseinheit 120 kann für die Durchführung zusätzlicher Sicherungsroutinen in Verbindung mit weiteren miteinander verschalteten Funktionseinheiten 12, 13 programmiert sein. Das Signalmittel 107, 108 wird zur Zustandsunterscheidung entsprechend angesteuert. Ein separates Sicherheitsgehäuse, daß nahe an der Vergußmasse 105 und ringsherum angeordnet ist, kann eingespart werden, wenn das Meter bereits ein Sicherheitsgehäuse aufweist, d.h. daß das umgebende Sicherheitsgehäuse Bestandteil eines Meters 1 ist. Das Signalmittel 107, 108 ragt in demjenigen Bereich des Sicherheitsmoduls 100 durch das Vergußmaterial 105 hindurch, wo das umgebende Metergehäuse zur Signalisierung des Modulzustandes eine Öffnung 109 aufweist, welche .sich zur Bedienoberfläche 88, 89 des Meters 1 erstreckt. Die Abmaße bzw. der Durchmesser der Öffnung liegen in der Größenordnung des Signalmittels, welches zum Beispiel als Anzeigeeinheit realisiert ist. Eine solche Anzeigeeinheit kann eine oder mehrere oder mehrfarbige Leuchtdioden (LED´s) einschließen. Letztere können zur Zustandsunterscheidung auch blinkend gesteuert werden. Wenn die Leuchtdioden LED´s 107, 108 zur Zustandsunterscheidung gleichzeitig angesteuert werden, hat deren emittiertes sichtbares Licht eine kombinierte Farbe (beispielsweise Orange), die im Ergebnis der Authorisierungsroutine beim dynamischen Selbsttest einen Fehler signalisiert.

Die in der Figur 2 gezeigten Speicher 114 und SRAM 116 werden nachfolgend zur Vereinfachung mit NVRAM_A bezeichnet. Im NVRAM_A sind zum Zeitpunkt t_i beispielsweise Ascending-, Descending-, Stückzahl- und weitere Daten gegeben, die für zukünftige Abrechnungen genutzt

werden sollen. Vereinfachend wird die Zusammenfassung der vorgenannten Daten auch als P'_{ti} = Postregistersatz bezeichnet. Dabei bedeutet das Zeichen „' „ hinter dem Buchstaben P, daß dieser Postregistersatz vom ASIC 150 berechnet wurde. Jeder Postregistersatz wird außerdem mit einem MAC abgesichert, welcher vom Modulprozessor 120 berechnet wurde und ebenfalls im NVRAM_A gespeichert vorliegt.

Der in der Figur 2 gezeigte batteriegestützte statische RAM 124 des OTP-Prozessorbausteins 120 wird nachfolgend mit NVRAM_P bezeichnet, weil OTP-intern nichtflüchtig gespeicherten Daten nicht von außen lesbar sind. Eine von der Batterie 134 über den Umschalter 180 und über die Spannungsüberwachungseinheit 12 gelieferte Spannung Ub+ ist auf der Leitung 138 ständig verfügbar und versorgt den OTP-internen Speicher RAM 124, der dadurch Daten nichtflüchtig speichern kann. Ein bereits früher eingegebener Portowert bleibt somit nichtflüchtig gespeichert, bis er überschrieben wird. Gegeben sei deshalb zum Zeitpunkt t_i im NVRAM_A oder NVRAM_P ein Portowert p_{ti}, der für zukünftige Abrech-nungen genutzt werden kann. Eine Abrechnung $P_{t(i+1)} = F(P'_{t(i-1)}, p_{ti}) = P_{neu}$ bedeutet, daß zum Zeitpunkt t_{i-1} bereits ein Postregistersatz vorlag, der berücksichtigt wird, wenn Zeitpunkt t_i ein Portowert p_{ti} eingegeben wird und daß die Abrechnung nach der Funktion F zum Zeitpunkt t_{i+1} vom Modulprozessor 120 vorgenommen wurde. Anderenfalls bedeutet eine Abrechnung $P'_{t(i+1)} = F'(P'_{t(i-1)}, p_{ti})$, daß die Abrechnung nach der Funktion F' zum Zeitpunkt t_{i+1} von der Hardwareabrecheneinheit des ASIC's 150 vorgenommen wurde.

Zur Authorisierungsprüfung an einem beliebigen Zeitpunkt t_i können die Daten des Postregistersatz aus einem NVRAM_A verwendet werden, um einen MAC vom Postregistersatz zu bilden. Wenn der Ausdruck $MAC(P_{ti})$ aber kein Zeichen „' „ hinter dem Buchstaben P hat, dann bedeutet dies, daß dieser Postregistersatz und MAC vom Modulprozessor 120 zum Zeitpunkt t_i berechnet wurde. Der Mikroprozessor kann im NVRAM_P erforderlichenfalls sofort berechnen:

$P_{t(i+1)}$ = Postregistersatz zum Zeitpunkt t_{i+1}

$MAC(P_{t(i+1)})$ = MAC vom Postregistersatz zum Zeitpunkt t_{i+1}

Die Figur 7 zeigt eine Darstellung von Abläufen bei der Abrechnung anhand eines Zeitstrahles. Die Eingabe eines neuen Portowertes oder eine Briefanlage bildet den Ausgangspunkt t_0 für eine Anzahl an Abläufen. Bei Briefanlage kann auch von der Weiterverwendung eines bereits eingegebenen Portowertes als neuen Portowert ausgegangen werden. Zunächst wird vom Modulprozessor 120 aus dem NVRAM_A ein MAC_{alt} geholt und definiert durch den Zeitpunkt t_0 als $MAC(P_{to})$ im NVRAM_P gespeichert. Zugleich werden die P'_{ti}–Registerdaten zu einem MAC verarbeitet, wobei das Ergebnis spätestens zum Zeitpunkt t_1 vorliegt und ebenfalls im NVRAM_P zwischengespeichert wird. Dann wird der zum Zeitpunkt t_1 vorliegende $MAC(P'_{to})$ mit dem $MAC(P_{to})$ verglichen. Bei Übereinstimmung liegt kein Fehler vor und es wird vom Modulprozessor 120 das Ende der Eingabe zum Zeitpunkt t_2 abgewartet. Der Modulprozessor 120 stößt zum Zeitpunkt t_2 eine Vorausberechnung eines neuen Postregistersatzes P_{t2} und eine weitere Bildung eines neuen MAC an, wobei der Wert des MAC_{neu} gespeichert wird. Der Vorgang ist zum Zeitpunkt t_3 abgeschlossen und nun wird eine an sich bekannte Abrechnung und Bildung eines neuen Postregistersatzes vom ASIC 150 vorgenommen. Während der Postregistersatz P'_{t3} gebildet wird, liegen zwei MAC´s gespeichert vor, nämlich MAC_{alt} = $MAC(P_{to})$ und der vorausberechnete MAC_{neu} = $MAC(P_{t2})$. Davor gilt noch der alte MAC_{alt} und bei Spannungsausfall kann auf die vorherigen Daten zurückgegriffen werden, welche im NVRAM_A gespeichert vorliegen. Die Abrechnung wird dann vollständig wiederholt. Somit ergibt sich für einen eventuellen Manipulator zu keinem Zeitpunkt eine Fälschungsmöglichkeit. Ist der Postregistersatz P'_{t3} zum Zeitpunkt t_4 vom ASIC berechnet worden, dann erfolgt ein Löschen bzw. Überschreiben des alten $MAC(P_{to})$ mit dem

neuen MAC(P_{t2}) und ein Speichern des neuen Registersatzes P'_{t3} im NVRAM_A. Letzterer Vorgang ist zum Zeitpunkt t_5 abgeschlossen.

Anhand des - in der Figur 8 dargestellten - Flußdiagramms werden nun die Prüfungen näher erläutert, welche im System vor dem Frankieren ablaufen. Der Mikroprozessor CPU 121 ist durch ein entsprechendes im Flash 128 gespeichertes Programm programmiert, solche vorgenannten Selbsttests auszuführen, wobei nach dem Start 299, in einem ersten Schritt 300 ein Power on-Selbsttest durchgeführt und dann im Schritt 301 gefragt wird, ob der Power on-Selbsttest ein OK ergeben hat. Ist das der Fall, so wird im Schritt 302 die grüne LED 107 vom Mikroprozessor CPU 121 über ein I/O-Port 125 leuchtend gesteuert. Anderenfalls wird im Schritt 303 die rote LED 108 vom Mikroprozessor CPU 121 über ein I/O-Port 125 leuchtend gesteuert.

Vom Schritt 302 wird auf die Abfrage 304 verzweigt, in welcher geprüft wird, ob eine weitere statische Prüfung verlangt wird. Ist das der Fall, so wird zum Schritt 300 zurückverzweigt. Anderenfalls wird auf die Abfrage 305 verzweigt, in welcher geprüft wird, ob durch einen Briefsensor eine Briefanlage festgestellt bzw. vom Modulprozessor 120 eine Eingabe einen neuen Portowertes erkannt wird. Ist dies beides nicht der Fall, dann wird auf den Schritt 302 zurückverzweigt und somit eine Warteschleife solange durchlaufen, bis eine Briefanlage/Neueingabe festgestellt worden ist. Im letzteren Fall wird auf den Schritt 306 verzweigt, um das Eingeben der Daten zu beenden. Gleichzeitig oder kurz nach dem Zeitpunkt t_0 beginnend, wird ein Schritt 307 zur MAC-Berechnung auf der Grundlage der zum Zeitpunkt t_0 verfügbaren Postregisterdaten P'_{to} gestartet. Ein vom OTP bereits früher gebildeter MAC(P_{to}) ist zum Zeitpunkt t_0 gültig. Die MAC-Berechnung ist zum Zeitpunkt t_1 abgeschlossen. Der berechnete MAC(P'_{to}) wird mit dem alten zum Zeitpunkt t_0 gültigen (vom OTP bereits früher gebildeten) MAC(P_{to}) zum Zeitpunkt t_1 im Schritt 308 verglichen. Bei Nichtübereinstimmung wird zum Schritt 315 verzweigt, um die LED's 107, 108 orange leuchtend zu steuern. Anderenfalls wird zu den Schritten

309, 310 verzweigt. Dort erfolgt zum Zeitpunkt t_2 im OTP 120 eine Vorausberechnung des neuen Postregistersatzes P_{t2} und anschließend eine MAC-Bildung, ggf. mit Speicherung des MAC(P_{t2}) im NVRAM_P.

Zum Zeitpunkt t_3, wenn im Schritt 311 die Speicherung des MAC(P_{t2}) im NVRAM_P von der einen Datenverarbeitungseinheit 120 abgeschlossen worden ist, wird vom anderen Datenverarbeitungseinheit, nämlich von einer – nicht gezeigten – Hardware-Abrecheneinheit im ASIC 150 eine Berechnung des neuen Postregistersatzes im Schritt 312 durchgeführt.

In einem abschließenden Schritt 313 erfolgt wieder eine Abspeicherung der Ergibnisse P'_{t3} und MAC(P_{t2}) im NVRAM_A. In Vorbereitung eines Frankierens können dann noch eine Anzahl von weiteren Schritten durchlaufen werden, mindestens jedoch ein Schritt 314 Druckdatenbereitstellung zum Frankieren des Briefes. Anschließend wird zum Schritt 302 zurückverzweigt.

Der Schritt 314 mit Druckdatenbereitstellung zum Frankieren kann optional einen – nicht gezeigten - Subschritt zum Übermitteln eines generierten Sicherheitscodes.einschließen. Zum Generieren des Sicherheitscode wird zwar ebenfalls eine prinzipiell vergleichbare Bildungsprozedure genutzt, wie bei der MAC-Bildung, der Daten-Authorisierungs-Code DAC setzt sich aber aus anderen Daten zusammen und das Generieren erfolgt zu einem anderem Zeitpunkt t_{i+1} ab Dateneingabeende zu einem Wert DAC($P_{t(i+1)}$,sonstige Daten).

Der Modulprozessor 120 arbeitet mit einem – nicht gezeigten - Steuerungsprozessor des Meters zusammen, wobei letzterer den Sicherheitscode empfängt, die Druckdaten zusammenstellt und zum Druckkopf übermittelt.

Dadurch, daß nach dem Abspeichern der Ergebnisse zum Schritt 302 zurückgezweigt wird, ergibt sich on demand eine zweistufige Prüfung. Im Fehlerfall im Ergebnis der dynamischen Prüfung werden im Schritt 309 beide, die grüne LED 107 und die rote LED 108, vom Mikroprozessor

CPU 121 über ein I/O-Port 125 leuchtend gesteuert. Somit ergibt sich der Gesamteindruck, daß die LED´s orange leuchten.

Die in der Figur 8 auf der rechten Hälfte des Flußplanes vermerkten Zeitpunkte t_0 bis t_5 sollen helfen, einen Bezug zur Figur 7 herzustellen. Damit sollen alternative Abläufe jedoch nicht ausgeschlossen werden. Die Vorausberechnung muß nicht nach einer Authorisierungsüberprüfung erfolgen. Ebensogut kann zuerst ein neuer Postregistersatz P_{ti} vom Modulprozessor 120 vorausberechnet werden, wobei ein bereits eingegebener gespeicherter Portowert p_t berücksichtigt wird. Erst danach wird vom Modulprozessor 120 eine Authorisierungsüberprüfung bezüglich des alten im Speicher NVRAM_A gespeicherten Postregistersatzes P'_{ti-1} vorgenommen, wobei ein Authorisierungscode $MAC(P'_{t(i-1)})$ vom Modulprozessor gebildet und mit einem zugehörigen im Speicher NVRAM_A gespeicherten bisherigen Authorisierungscode $MAC_{alt} = MAC(P_{t(i-1)})$ verglichen wird. Nach der Authorisierungsüberprüfung berechnet der Modulprozessor 120 einen neuen Authorisierungscode $MAC_{neu} = MAC(P_{ti})$ über den neuen Postregistersatz P_{ti}. Der neue Postregistersatz P_{ti} bleibt bis zur MAC-Berechnung im OTP-internen NVRAM_P gespeichert. Das ist wichtig, um eine Manipulation während der Berechnung zu verhindern, insbesondere wenn die Vorausberechnung des neuen Postregistersatz P_{ti} und des neuen MAC´s zeitlich auseinander liegen.

Im NVRAM_A können zu einem Zeitpunkt t_i also folgende Daten gespeichert sein:

P'_{ti-1} - bisheriger Postregistersatz, der vom ASIC berechnet wurde,

$MAC(P_{ti-1})$ - zugehöriger MAC_{alt} über einen gleichen Postregistersatz, der beim vorherigem Abrechnen vom Modulprozessor vorausberechnet wurde.

Im Speicher NVRAM_P speichert die erste Datenverarbeitungseinheit, vorzugsweise der Modulprozessor 120, zu dem ersten Zeitpunkt t_i gegebenenfalls folgende Daten:

$$MAC(P_{ti}) = MAC_{neu}$$

Von der zweiten Datenverarbeitungseinheit, vorzugsweise vom ASIC 150, wird zu einem späteren zweiten Zeitpunkt t_{i+1} die Abrechung mit einem Portowert p_{ti} nach der Abrechnungsfunktion F´ durchgeführt. Es erfolgt:

1. Bilden des Postregistersatzes $P'_{t(i+1)} = F'(P'_{t(i-1)} , p_{ti})$ mit anschließender Speicherung im Speicher NVRAM_A.
2. Außerdem überschreibt der Modulprozessor 120 den im NVRAM_A gespeicherten $MAC(P_{ti-1})_{alt}$ mit dem vorausberechneten im NVRAM_P gespeicherten $MAC(P_{ti})_{neu}$.
3. Optional übermittelt der Modulprozessor 120 einen zusätzlich generierten Sicherheitscode $DAC(P_{t(i+1)}$,sonstige Daten) zur extern vom Sicherheitsmodul im Meter angeordneten dritten Datenverarbeitungseinheit (nicht gezeigt) zur Druckbilderzeugung.

Vor dem nächsten Frankieren wiederholt sich der Vorgang. Bis zum Zeitpunkt t_{i+2} wird ein neuer Portowert p_{ti+2} eingegeben. Zum Zeitpunkt t_{i+2} oder später kann wieder die Manipulationsfreiheit von $P'_{t(i+1)}$ geprüft werden, indem $MAC(P'_{t(i+1)})$ berechnet und mit dem im NVRAM_A gespeicherten Wert $MAC(P_{ti})_{alt}$ verglichen wird. Es kann aber auch schon optional eine Generierung eines zusätzlichen Sicherheitscodes $MAC(P_{t(i+1)}$,sonstige Daten) begonnen werden. Vor der eigentlichen Abrechnung durch den ASIC 150 erfolgt wieder eine MAC-Vorausberechnung durch den Modulprozessor. Zum Beispiel errechnet der Modulprozessor im Zeitpunkt t_{i+3} einen neuen Authorisierungscode:

$$MAC_{neu} = MAC(P_{t(i+3)}) = MAC[F(P'_{t(i+1)} , p_{t(i+2)})].$$

Erfindungsgemäß ist in einer Subvariante vorgesehen, daß der aufgrund des vorausberechneten neuen Postregistersatzes gebildete zugehörigen Authorisierungscode MAC_{neu} nach seiner Erzeugung in einem Bereich des nichtflüchtigen Speichers 114, 116 (NVRAM_A für die Postregisterdaten) gespeichert wird. Alternativ oder zusätzlich kann der aufgrund des

vorausberechneten neuen Postregistersatzes gebildete zugehörigen Authorisierungscode MAC_{neu} nach seiner Erzeugung in einem Bereich des internen nichtflüchtigen Speichers 124 (NVRAM_P) der ersten Datenverarbeitungseinheit 120 (Modulprozessor) gespeichert werden.

Es ist in einer Subvariante vorgesehen, daß in Verbindung mit der Speicherung des von der zweiten Datenverarbeitungseinheit 150 (ASIC) ermittelten neuen Postregistersatzes $P'_{t(i+1)}$ und des vorausberechneten neuen Authorisierungscode $MAC(P_{ti})_{neu}$ in den nichtflüchtigen Speichern 114, 116 (NVRAM_A) letzterer Authorisierungscode in einem weiteren Bereich des internen nichtflüchtigen Speichers 124 (NVRAM_P) der ersten Datenverarbeitungseinheit 120 (Modulprozessor) gespeichert wird, so daß der zu dem neuen Postregistersatz zugehörige Authorisierungscode bis zur nächsten Abrechnung redundant gespeichert ist.

Erfindungsgemäß ist das Sicherheitsmodul zum Einsatz in postalischen Geräten bestimmt, insbesondere zum Einsatz in einer Frankiermaschine. Jedoch kann das Sicherheitsmodul auch eine andere Bauform aufweisen, die es ermöglicht, daß es beispielsweise auf die Hauptplatine eines Personalcomputers gesteckt werden kann, der als PC-Frankierer einen handelsüblichen Drucker ansteuert.

Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Anordnungen bzw. Ausführungen der Erfindung entwickelt bzw. eingesetzt werden können, die - vom gleichen Grundgedanken der Erfindung ausgehend - von den anliegenden Schutzansprüchen umfaßt werden.

***

Zusammenfassung

Die Erfindung betrifft ein Sicherheitsmodul mit einer ersten und zweiten Datenverarbeitungseinheit (120, 150), mit nichtflüchtigen Speichern (114, 116) für Postregisterdaten und Verfahren zur Sicherung der Postregisterdaten vor Manipulation. Zu einem ersten Zeitpunkt t_i, mindestens nach Briefanlage und nach einer Überprüfung der bisher gültigen Abrechnungsdaten anhand eines Authorisierungscodes MAC_{alt}, nimmt die erste Datenverarbeitungseinheit (120) eine Vorausberechnung des neuen Postregistersatzes vor, der sich unter Berücksichtigung des zuvor eingestellten Portowertes ergibt, und bildet einen neuen Authorisierungscode MAC_{neu}. Zu einem zweiten Zeitpunkt t_{i+1}, nimmt die zweite Datenverarbeitungseinheit (150) eine Abrechnung mit Berechnung des neuen Postregistersatzes vor, der sich unter Berücksichtigung des eingestellten Portowertes ergibt. Abschließend erfolgt eine Speicherung des vorausberechneten neuen Authorisierungscode MAC_{neu} und des von der zweiten Datenverarbeitungseinheit (150) ermittelten neuen Postregistersatzes in den nichtflüchtigen Speichern (114, 116).

Fig. 7

***

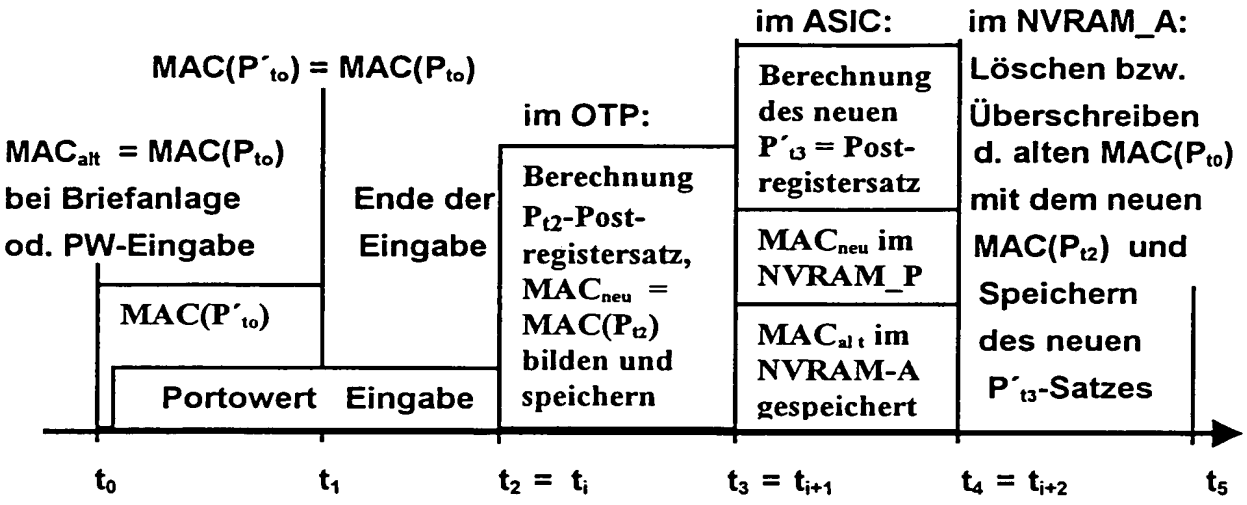
im ASIC:
im NVRAM_A:
MAC(P´to) = MAC(Pto)
im OTP:
Berechnung des neuen P´t3 = Post-registersatz
Löschen bzw. Überschreiben d. alten MAC(Pt0) mit dem neuen MAC(Pt2) und Speichern des neuen P´t3-Satzes
MACalt = MAC(Pto) bei Briefanlage od. PW-Eingabe
Ende der Eingabe
Berechnung Pt2-Post-registersatz, MACneu = MAC(Pt2) bilden und speichern
MACneu im NVRAM_P
MAC(P´to)
MACalt im NVRAM-A gespeichert
Portowert Eingabe
t0
t1
t2 = ti
t3 = ti+1
t4 = ti+2
t5

Fig. 7

Patentansprüche

1.Sicherheitsmodul zur Sicherung der Postregister vor Manipulation, mit einem Programmspeicher (128), einer ersten und zweiten Datenverarbeitungseinheit (120, 150), mit nichtflüchtigen Speichern (114, 116), welche operativ miteinander verbunden sind, um mindestens die zweite Datenverarbeitungseinheit (150) zu veranlassen, die Abrechnung durchzuführen und um in dem nichtflüchtigen Speicher (114, 116) die Postregisterdaten zu speichern , gekennzeichnet dadurch, daß die erste Datenverarbeitungseinheit (120) einen internen nichtflüchtigen Speicher (124) aufweist, in welchem mindestens ein Schlüssel für die Berechnung eines Authorisierungscodes vor einem Zugriff geschützt gespeichert ist, und wobei die erste Datenverarbeitungseinheit (120) durch ein Programm im Programmspeicher (128) programmiert ist:

- einen Postregistersatz vorauszuberechnen,
- einen zugehörigen Authorisierungscode (MAC) über den vorausberechneten Postregistersatz zu bilden und
- den vorausberechneten Authorisierungscode (MAC) zusammen mit den im Ergebnis der Abrechnung gebildeten Postregisterdaten im nichtflüchtigen Speicher (114, 116) zu speichern.

2. Sicherheitsmodul, nach Anspruch 1, gekennzeichnet dadurch, daß die erste Datenverarbeitungseinheit ein Modulprozessor (120) ist, welcher programmiert ist, einen neuen Postregistersatz entsprechend des eingegebenen oder bereits gespeicherten Portowertes vorauszuberechnen und darüber einen zugehörigen Authorisierungscode (MAC) zu bilden.

3. Sicherheitsmodul, nach den Ansprüchen 1 und 2, gekennzeichnet dadurch, daß die erste Datenverarbeitungseinheit (120) als Modulprozessor des Sicherheitsmoduls (100) für die Durchführung von mindestens einer Authorisierungsroutine für die Postregisterdaten programmiert ist, wobei deren festgestellte Authorisierung in Verbindung mit dem zugehörigen Authorisierungscode (MAC) im nichtflüchtigen Speichern (114, 116) einen Modulzustand signalisiert, welcher eine weitere Abrechnung durchzuführen gestattet, und wobei zur Signalisierung des Modulzustandes ein optisches oder akustisches Signalmittel (107, 108) am Modulprozessor (120) angeschlossen ist.

4. Sicherheitsmodul, nach den Ansprüchen 1 bis 3, gekennzeichnet dadurch, daß die erste Datenverarbeitungseinheit (120) als Modulprozessor des Sicherheitsmoduls (100) für die Durchführung zusätzlicher Sicherungsroutinen in Verbindung mit weiteren miteinander verschalteten Funktionseinheiten (12, 13) programmiert ist und daß zur Signalisierung des Modulzustandes ein optisches oder akustisches Signalmittel (107, 108) am Modulprozessor angeschlossen ist und von dem das Signalmittel (107, 108) zur Zustandsunterscheidung entsprechend unterschiedlich angesteuert wird.

5. Sicherheitsmodul, nach Anspruch 4, gekennzeichnet dadurch, daß das Signalmittel (107, 108) in demjenigen Bereich des Sicherheitsmoduls (100) durch eine Vergußmasse (105) hindurchragt, wo das umgebende Sicherheitsgehäuse zur Signalisierung des Modulzustandes eine Öffnung (109) aufweist, daß das umgebende Sicherheitsgehäuse Bestandteil eines Meters (1) ist und sich die Öffnung (109) zur Bedienoberfläche (88, 89) des Meters (1) erstreckt, wobei die Abmaße bzw. der Durchmesser der Öffnung in der Größenordnung des Signalmittels liegen.

6. Sicherheitsmodul, nach einem der Ansprüche 1 bis 5, gekennzeichnet da durch, daß das Signalmittel als Anzeigeeinheit realisiert ist.

7. Sicherheitsmodul, nach Anspruch 6, gekennzeichnet dadurch, daß die Anzeigeeinheit eine oder mehrere oder mehrfarbige Leuchtdioden (LED´s) einschließt.

8. Sicherheitsmodul, nach Anspruch 7, gekennzeichnet dadurch, daß die Leuchtdioden LED´s (107, 108) zur Zustandsunterscheidung blinkend gesteuert werden.

9. Sicherheitsmodul, nach Anspruch 7, gekennzeichnet dadurch, daß die Leuchtdioden LED´s (107, 108) zur Zustandsunterscheidung gleichzeitig angesteuert werden, wobei deren emittiertes sichtbares Licht eine kombinierte Farbe hat, die im Ergebnis der Authorisierungsroutine beim dynamischen Selbsttest einen Fehler signalisiert.

10. Verfahren zur Sicherung der Postregister vor Manipulation, mit einer Authorisierungscode-Berechnung und Abrechnung durch eine erste und eine zweite Datenverarbeitungseinheit eines Sicherheitsmoduls, gekennzeichnet durch die Schritte:

- Vorausberechnung des neuen Postregistersatzes (P_{ti}) mittels der ersten Datenverarbeitungseinheit (120), zu einem ersten Zeitpunkt (t_i) mindestens nach Briefanlage, wobei sich der neue Postregistersatz unter Berücksichtigung des zuvor eingestellten Portowertes (p_{ti-1}) ergibt, und Bilden eines neuen Authorisierungscodes ($MAC(P_{ti})_{neu}$) nach einer Authorisierungsüberprüfung des bisher gültigen Postregistersatzes aus einer vorhergehenden Abrechnung mittels eines bisher zugeordneten Authorisierungscodes (MAC_{alt}),
- Abrechnung mit Berechnung des neuen Postregistersatzes ($P'_{t(i+1)}$) zu einem zweiten Zeitpunkt (t_{i+1}), mittels der zweiten Datenverarbeitungseinheit (150), wobei sich der neue Postregistersatz unter Berücksichtigung des eingestellten Portowertes ($_{ti-1}$) ergibt, und
- Speicherung des vorausberechneten neuen Authorisierungscode ($MAC(P_{ti})_{neu}$) und des von der zweiten Datenverarbeitungseinheit (150) ermittelten neuen Postregistersatzes ($P'_{t(i+1)}$) in den nichtflüchtigen Speichern (114, 116).

11. Verfahren, nach Anspruch 10, gekennzeichnet dadurch, daß der aufgrund des vorausberechneten neuen Postregistersatzes (P_{ti}) gebildete zugehörigen Authorisierungscode ($MAC(P_{ti})_{neu}$) nach seiner Erzeugung in einem Bereich des nichtflüchtigen Speichers (114, 116) für die Postregisterdaten gespeichert wird.

12. Verfahren, nach Anspruch 10, gekennzeichnet dadurch, daß der aufgrund des vorausberechneten neuen Postregistersatzes (P_{ti})

gebildete zugehörigen Authorisierungscode ($MAC(P_{ti})_{neu}$) nach seiner Erzeugung in einem Bereich des internen nichtflüchtigen Speichers (124) der ersten Datenverarbeitungseinheit (120) gespeichert wird.

13. Verfahren, nach Anspruch 10, gekennzeichnet dadurch, daß in Verbindung mit der Speicherung des von der zweiten Datenverarbeitungseinheit (150) ermittelten neuen Postregistersatzes ($P'_{t(i+1)}$) und des vorausberechneten neuen Authorisierungscode ($MAC(P_{ti})_{neu}$) in den nichtflüchtigen Speichern (114, 116) letzterer Authorisierungscode in einem weiteren Bereich des internen nichtflüchtigen Speichers (124) der ersten Datenverarbeitungseinheit (120) gespeichert wird, so daß der zu dem neuen Postregistersatz zugehörige Authorisierungscode bis zur nächsten Abrechnung redundant gespeichert ist.

14. Verfahren, nach einem der Ansprüche 10 bis 13, gekennzeichnet dadurch, daß ein Modulprozessor (120) den in den nichtflüchtigen Speichern (114, 116, NVRAM_A) gespeicherten alten Authorisierungscode (MAC_{alt}) mit dem im internen Speicher (124, NVRAM_P) gespeicherten vorausberechneten neuen Authorisierungscode ($MAC(P_{ti})_{neu}$) überschreibt.

15. Verfahren, nach den Ansprüchen 10 bis 14, gekennzeichnet dadurch, daß der Modulprozessor (120) einen zusätzlichen Sicherheitscode $MAC(P_{t(i+1)},$ sonstige Daten) generiert und zur extern vom Sicherheitsmodul erfolgenden Druckbilderzeugung übermittelt.

*****

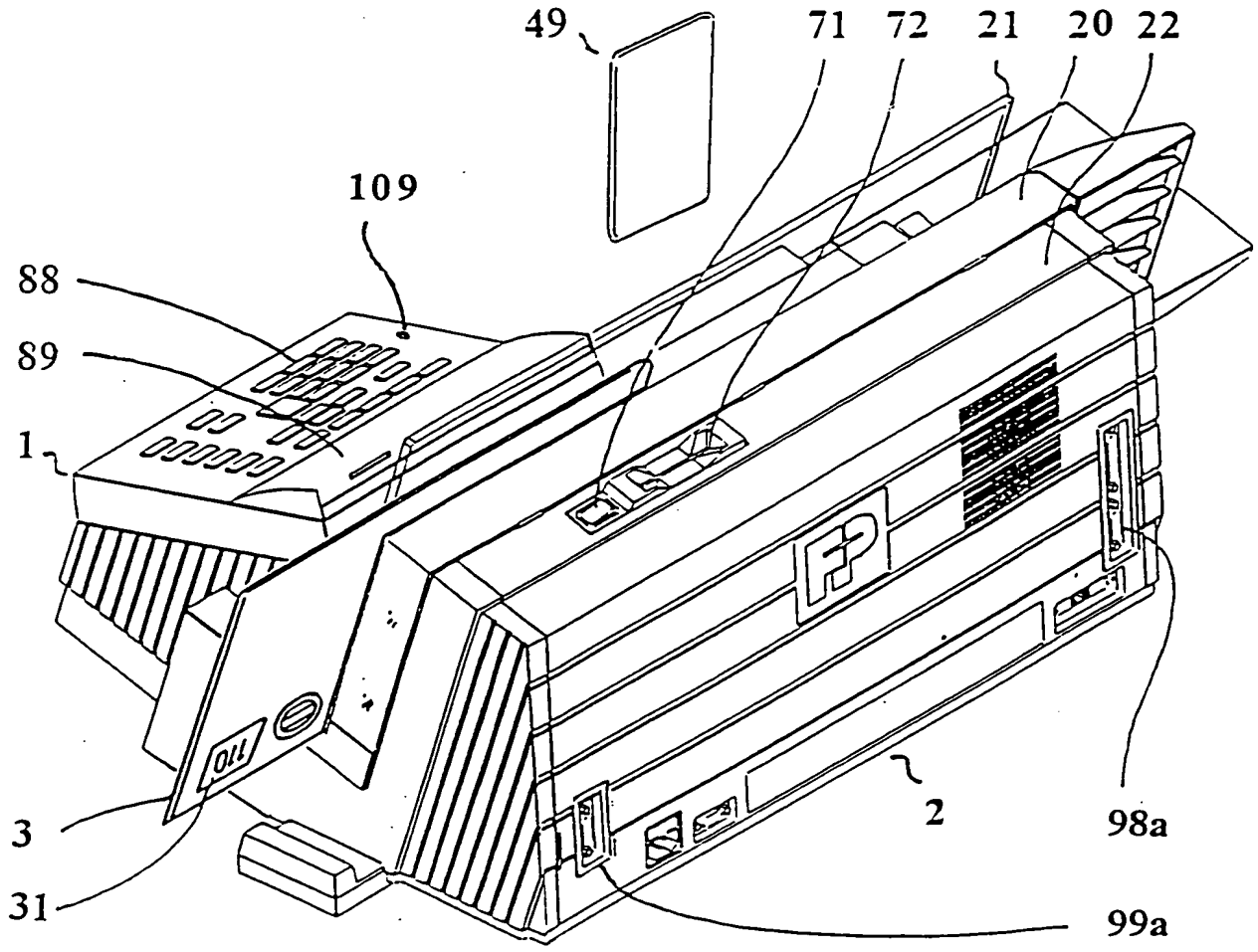

Fig. 1

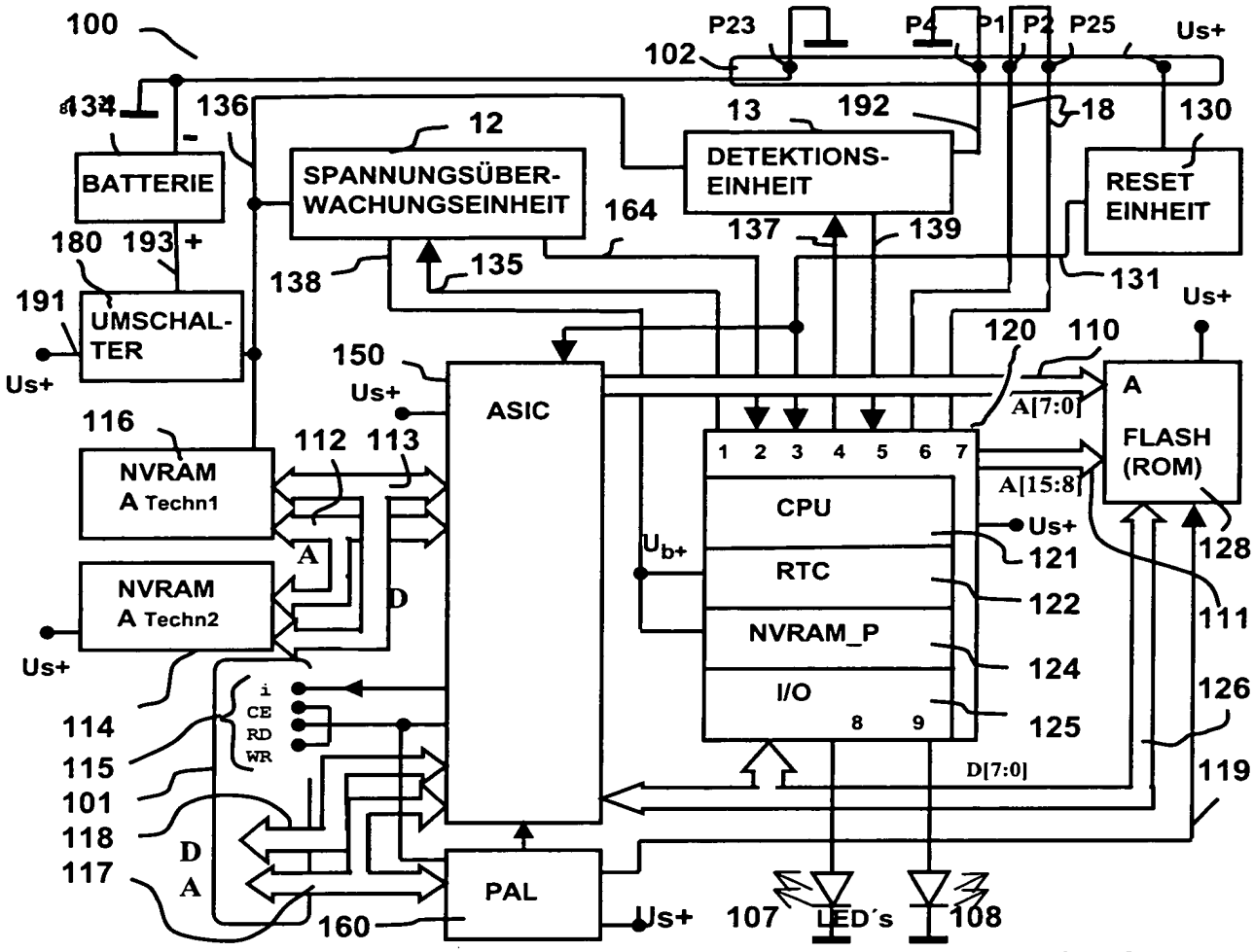
100
102
P23
P4
P1
P2
P25
Us+
134
136
12
13
192
18
130
BATTERIE
SPANNUNGSÜBER-
WACHUNGSEINHEIT
DETEKTIONS-
EINHEIT
RESET
EINHEIT
164
180
193
+
137
139
135
138
131
191
UMSCHAL-
TER
Us+
120
110
150
Us+
ASIC
A
FLASH
(ROM)
A[7:0]
116
112
113
1 2 3 4 5 6 7
NVRAM
A Techn1
A[15:8]
CPU
Us+
121
128
U_{b+}
RTC
122
111
NVRAM
A Techn2
NVRAM_P
124
126
Us+
I/O
125
8 9
i
CE
RD
WR
D[7:0]
119
114
115
101
118
117
D
A
PAL
160
Us+
107
LED´s
108

Fig. 2

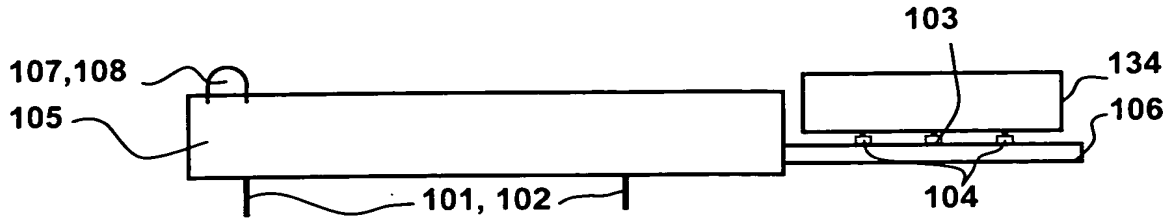

Fig. 3

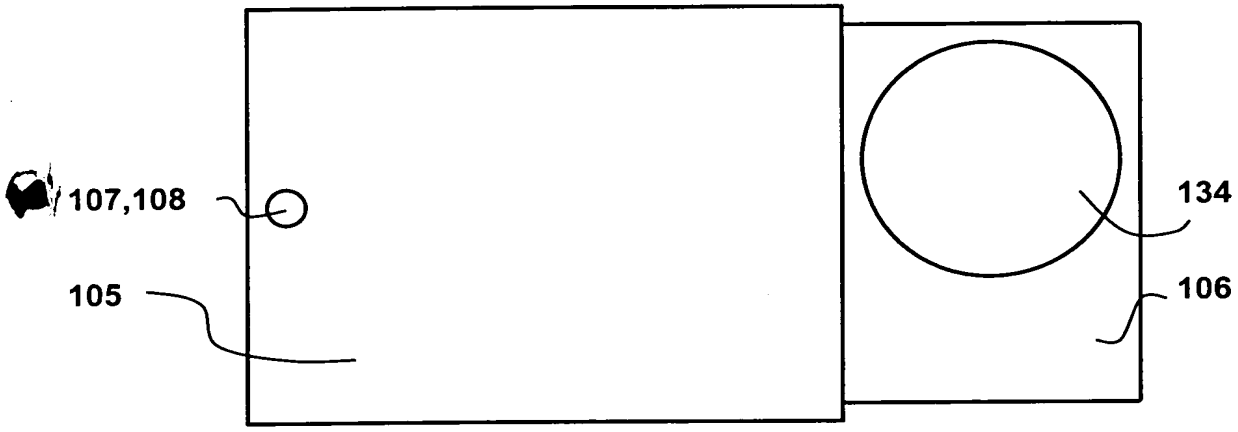

Fig. 4

Zustand Nr:	LEDs	leuchtet	blinkt	Aus	Anzeige	Bedeutung
220	R			X	Grün - leuchtend	OK
	G	X				
230	R	X			Rot - leuchtend	Fehler
	G			X		
240	R	X			Orange - leuchtend	Dyn. Fehler
	G	X				
250	R		X		Rot - blinkend	lange Zeit kein Kontakt zur DZ
	G			X		
260	R			X	Grün - blinkend	Schlüssel ist nicht installiert
	G		X			
270	R		X		Orange - blinkend	
	G		X			
280	R	X			Rot leuchtend Orange blinkend	
	G		X			
290	R		X		Grün leuchtend Orange blinkend	
	G	X				

Fig. 5

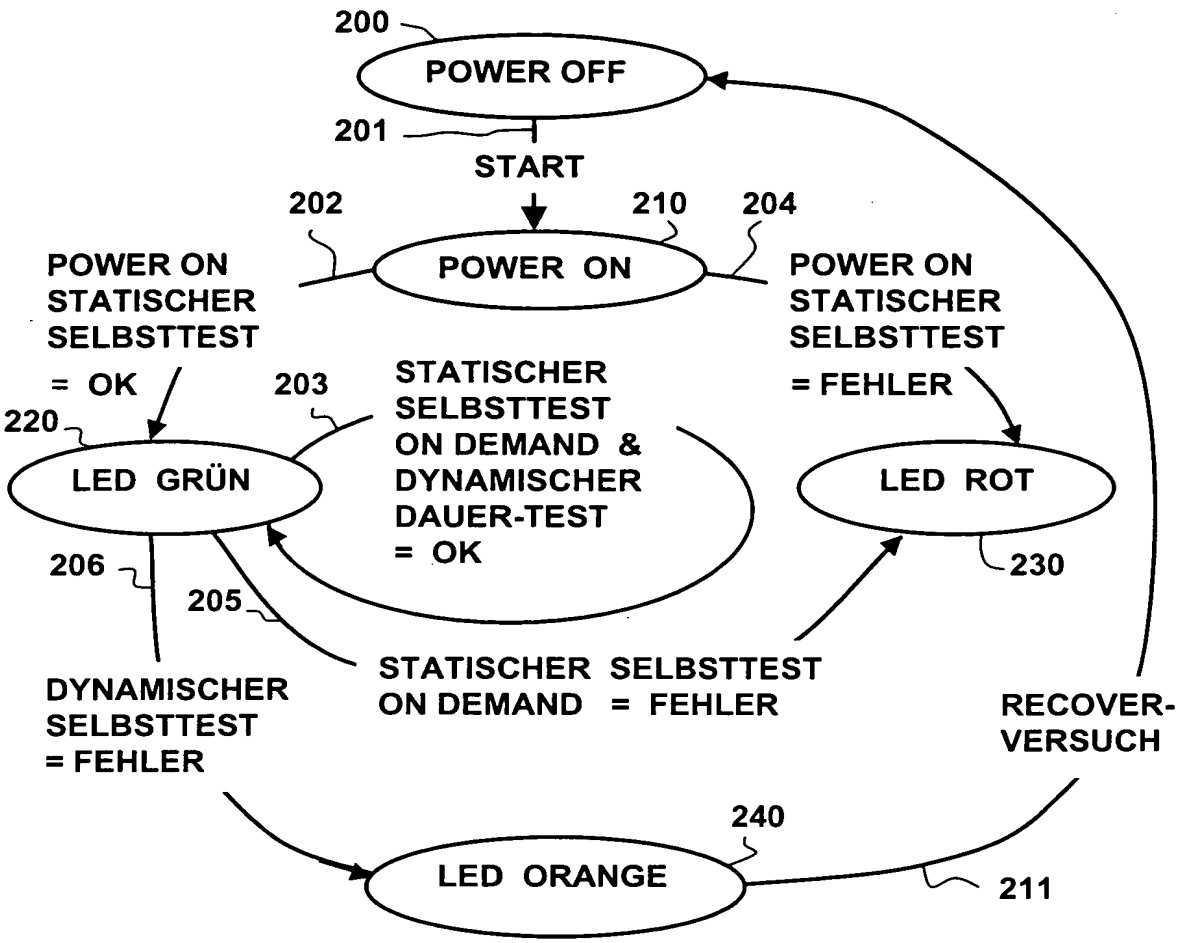
200
POWER OFF
201
START
202
210
204
POWER ON
POWER ON STATISCHER SELBSTTEST = OK
POWER ON STATISCHER SELBSTTEST = FEHLER
203
STATISCHER SELBSTTEST ON DEMAND & DYNAMISCHER DAUER-TEST = OK
220
LED GRÜN
LED ROT
230
206
205
DYNAMISCHER SELBSTTEST = FEHLER
STATISCHER SELBSTTEST ON DEMAND = FEHLER
RECOVER-VERSUCH
240
LED ORANGE
211

Fig. 6

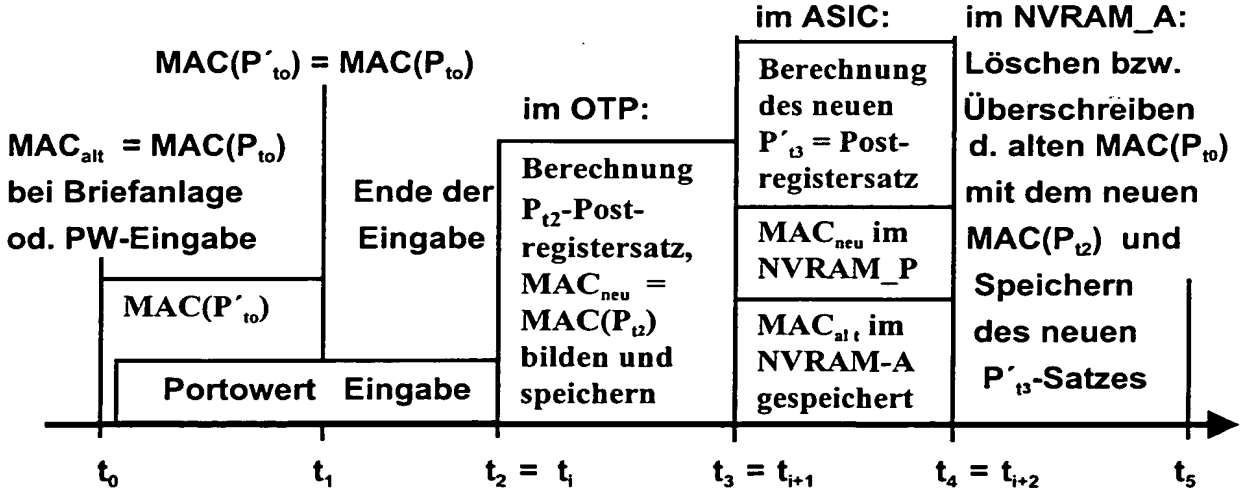
MAC(P´to) = MAC(Pto)
MACalt = MAC(Pto) bei Briefanlage od. PW-Eingabe
Ende der Eingabe
MAC(P´to)
Portowert Eingabe
im OTP:
Berechnung Pt2-Post-registersatz, MACneu = MAC(Pt2) bilden und speichern
im ASIC:
Berechnung des neuen P´t3 = Post-registersatz
MACneu im NVRAM_P
MACalt im NVRAM-A gespeichert
im NVRAM_A:
Löschen bzw. Überschreiben d. alten MAC(Pto) mit dem neuen MAC(Pt2) und Speichern des neuen P´t3-Satzes
t0
t1
t2 = ti
t3 = ti+1
t4 = ti+2
t5

Fig. 7

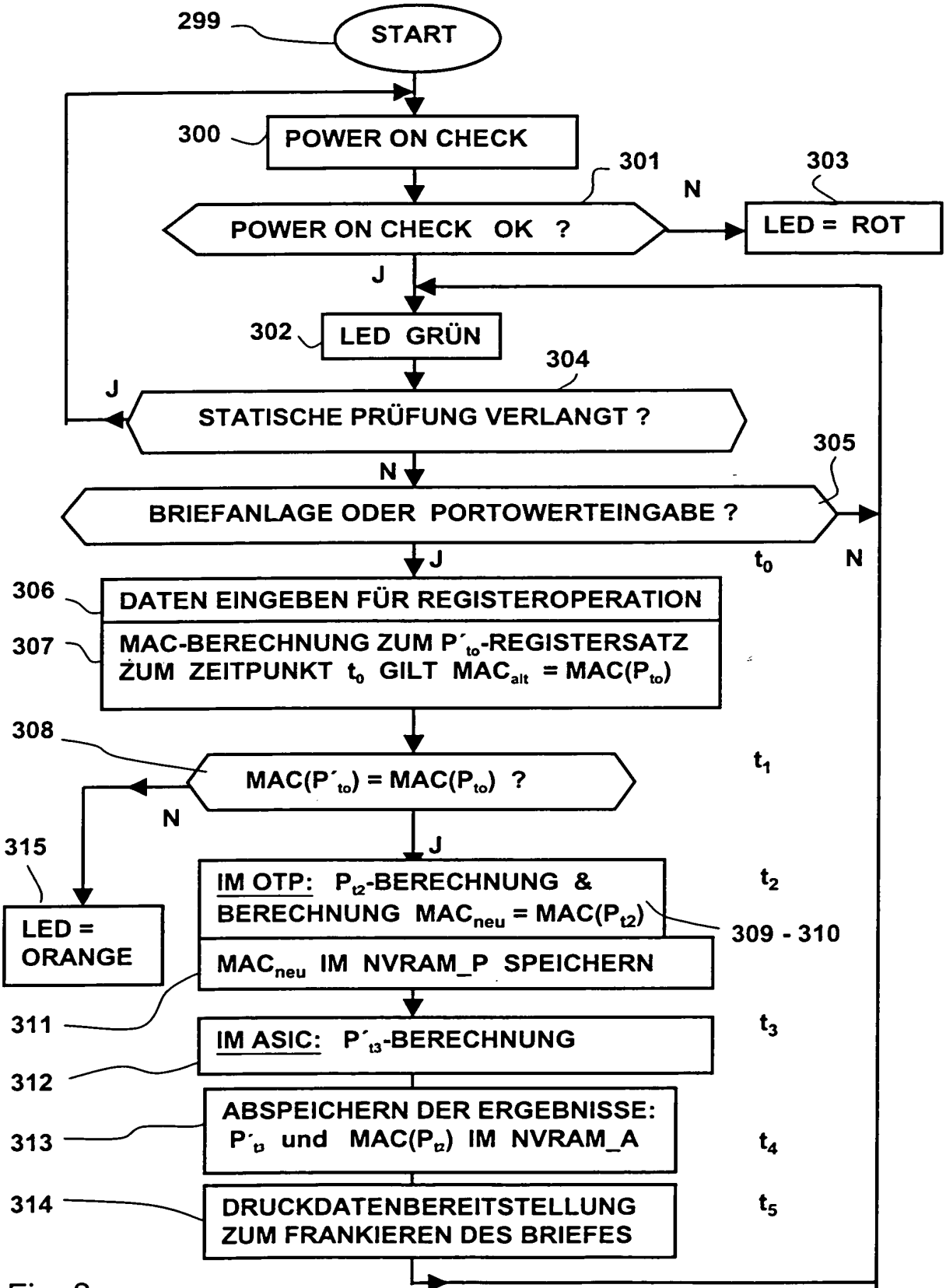
299
START
300
POWER ON CHECK
301
POWER ON CHECK OK ?
N
303
LED = ROT
J
302
LED GRÜN
304
J
STATISCHE PRÜFUNG VERLANGT ?
N
305
BRIEFANLAGE ODER PORTOWERTEINGABE ?
J
t0
N
306
DATEN EINGEBEN FÜR REGISTEROPERATION
307
MAC-BERECHNUNG ZUM P´to-REGISTERSATZ
ZUM ZEITPUNKT t0 GILT MACalt = MAC(Pto)
308
MAC(P´to) = MAC(Pto) ?
t1
N
J
315
LED = ORANGE
IM OTP: Pt2-BERECHNUNG &
BERECHNUNG MACneu = MAC(Pt2)
t2
309 - 310
MACneu IM NVRAM_P SPEICHERN
311
IM ASIC: P´t3-BERECHNUNG
t3
312
ABSPEICHERN DER ERGEBNISSE:
313
P´t3 und MAC(Pt2) IM NVRAM_A
t4
314
DRUCKDATENBEREITSTELLUNG
ZUM FRANKIEREN DES BRIEFES
t5

Fig. 8